Amendments to the Claims

Claim 1 (currently amended): A computer program product for providing end-to-end user authentication for legacy host application access, said computer program product embodied on a computer-readable medium readable by a computing device in a computing environment and comprising:

computer-readable program code means for establishing a secure session from a client machine to a server machine using a digital certificate transmitted from said client machine to said server machine, wherein said digital certificate represents ~~representing~~ said client machine or a user thereof;

computer-readable program code means for storing said transmitted digital certificate at said server machine;

computer-readable program code means for establishing a session from said server machine to a host system on behalf of said client machine, responsive to establishment of said secure session, using a legacy host communication protocol;

computer-readable program code means for passing said stored digital certificate from said server machine to a host access security system, responsive to receiving, at said server machine, a request from said host system for log-on information of said user;

computer-readable program code means, operable in said host access security system, for using said passed digital certificate to locate access credentials for said user;

computer-readable program code means for returning, from said host access security

system to said server machine, a user identifier associated with said located access credentials and either ~~accessing~~ a stored password or a generated password substitute representing said located credentials; and

computer-readable program code means for ~~using~~ forwarding said ~~stored~~ returned user identifier and password or ~~said generated~~ password substitute from said server machine to said host system as a response to said request for log-on information, such that said forwarded user identifier and password or password substitute can be used by said host system to transparently log said user on to a secure legacy host application executing at said host system, without requiring change to said host system.

Claim 2 (original): The computer program product as claimed in Claim 1, wherein said digital certificate is an X.509 certificate.

Claim 3 (currently amended): The computer program product as claimed in Claim 1 ~~or Claim 2~~, wherein said communication protocol is a 3270 emulation protocol.

Claim 4 (currently amended): The computer program product as claimed in Claim 1 ~~or Claim 2~~, wherein said communication protocol is a 5250 emulation protocol.

Claim 5 (currently amended): The computer program product as claimed in Claim 1 ~~or Claim 2~~, wherein said communication protocol is a Virtual Terminal protocol.

Claim 6 (original): The computer program product as claimed in Claim 3, wherein said host access security system is a Resource Access Control Facility (RACF) system.

Claim 7 (original): The computer program product as claimed in Claim 1, wherein said server machine is a Web application server machine.

Claim 8 (currently amended): A computer program product for providing end-to-end user authentication for legacy host application access, said computer program product embodied on a computer-readable medium readable by a computing device in a computing environment and ~~The computer program product as claimed in Claim 1, further~~ comprising:

computer-readable program code means for establishing a secure session from a client machine to a server machine using a digital certificate transmitted from said client machine to said server machine, wherein said digital certificate represents said client machine or a user thereof;

computer-readable program code means for storing said transmitted digital certificate at said server machine;

computer-readable program code means for establishing a session from said server machine to a host system on behalf of said client machine, responsive to establishment of said secure session, using a legacy host communication protocol;

computer-readable program code means for automatically sending a log-on message from said client machine to said server machine, responsive to receiving, at said client machine, a

request from said host system for log-on information of said user, wherein said log-on message uses placeholder syntax in place of a user identifier and a password of said user;

computer-readable program code means for passing said stored digital certificate from said server machine to a host access security system, responsive to receiving, at said server machine, said log-on message from said client machine;

computer-readable program code means, operable in said host access security system, for using said passed digital certificate to locate access credentials for said user;

computer-readable program code means for returning, from said host access security system to said server machine, a user identifier associated with said located access credentials and either a stored password or a generated password substitute representing said located credentials;

computer-readable program code means for modifying, by said server machine, said received log-on message by replacing said placeholder syntax with said returned user identifier and password or password substitute; and

computer-readable program code means for forwarding said modified log-on message from said server to said host system as a response to said request for log-on information, such that said user identifier and password or password substitute from said forwarded log-on message can be used by said host system to transparently log said user on to a secure legacy host application executing at said host system, without requiring change to said host system.

~~computer-readable program code means for requesting by said legacy host application, responsive to said computer-readable program code means for establishing said session, log-on information for said user;~~

~~computer-readable program code means for responding to said request for log on information by sending a log on message with placeholders from said client machine to said server machine, said placeholders representing a user identification and a password of said user; and~~

~~computer-readable program code means for substituting a user identifier associated with said located access credentials and said stored password or said generated passticket for said placeholders in said log on message.~~

Claim 9 (canceled)

Claim 10 (currently amended): A system for providing end-to-end user authentication for legacy host application access in a computing environment, comprising:

means for establishing a secure session from a client machine to a server machine using a digital certificate transmitted from said client machine to said server machine, wherein said digital certificate represents ~~representing~~ said client machine or a user thereof;

means for storing said transmitted digital certificate at said server machine;

means for establishing a session from said server machine to a host system on behalf of said client machine, responsive to establishment of said secure session, using a legacy host communication protocol;

means for passing said stored digital certificate from said server machine to a host access security system, responsive to receiving, at said server machine, a request from said host system for log-on information of said user;

means, operable in said host access security system, for using said passed digital certificate to locate access credentials for said user;

means for returning, from said host access security system to said server machine, a user identifier associated with said located access credentials and either ~~accessing~~ a stored password or a generated password substitute representing said located credentials; and

means for ~~using~~ forwarding said ~~stored~~ returned user identifier and password or ~~said generated~~ password substitute from said server machine to said host system as a response to said request for log-on information, such that said forwarded user identifier and password or password substitute can be used by said host system to transparently log said user on to a secure legacy host application executing at said host system, without requiring change to said host system.

Claim 11 (original): The system as claimed in Claim 10, wherein said digital certificate is an X.509 certificate.

Claim 12 (currently amended): The system as claimed in Claim 10 ~~or Claim 11~~, wherein said communication protocol is a 3270 emulation protocol.

Claim 13 (currently amended): The system as claimed in Claim 10 ~~or Claim 11~~, wherein said communication protocol is a 5250 emulation protocol.

Claim 14 (currently amended): The system as claimed in Claim 10 ~~or Claim 11~~, wherein said

communication protocol is a Virtual Terminal protocol.

Claim 15 (original): The system as claimed in Claim 12, wherein said host access security system is a Resource Access Control Facility (RACF) system.

Claim 16 (original): The system as claimed in Claim 10, wherein said server machine is a Web application server machine.

Claim 17 (currently amended): A system for providing end-to-end user authentication for legacy host application access in a computing environment, ~~The system as claimed in Claim 10, further~~ comprising:

means for establishing a secure session from a client machine to a server machine using a digital certificate transmitted from said client machine to said server machine, wherein said digital certificate represents said client machine or a user thereof;

means for storing said transmitted digital certificate at said server machine;

means for establishing a session from said server machine to a host system on behalf of said client machine, responsive to establishment of said secure session, using a legacy host communication protocol;

means for automatically sending a log-on message from said client machine to said server machine, responsive to receiving, at said client machine, a request from said host system for log-on information of said user, wherein said log-on message uses placeholder syntax in place of a

user identifier and a password of said user;

means for passing said stored digital certificate from said server machine to a host access security system, responsive to receiving, at said server machine, said log-on message from said client machine;

means, operable in said host access security system, for using said passed digital certificate to locate access credentials for said user;

means for returning, from said host access security system to said server machine, a user identifier associated with said located access credentials and either a stored password or a generated password substitute representing said located credentials;

means for modifying, by said server machine, said received log-on message by replacing said placeholder syntax with said returned user identifier and password or password substitute; and

means for forwarding said modified log-on message from said server to said host system as a response to said request for log-on information, such that said user identifier and password or password substitute from said forwarded log-on message can be used by said host system to transparently log said user on to a secure legacy host application executing at said host system, without requiring change to said host system.

~~means for requesting by said legacy host application, responsive to said means for establishing said session, log-on information for said user;~~

~~means for responding to said request for log on information by sending a log on message with placeholders from said client machine to said server machine, said placeholders representing~~

~~a user identification and a password of said user; and~~

~~means for substituting a user identifier associated with said located access credentials and said stored password or said generated passticket for said placeholders in said log on message.~~

Claim 18 (canceled)

Claim 19 (currently amended): A method for providing end-to-end user authentication for legacy host application access in a computing environment, comprising the steps of:

establishing a secure session from a client machine to a server machine using a digital certificate transmitted from said client machine to said server machine, wherein said digital certificate represents ~~representing~~ said client machine or a user thereof;

storing said transmitted digital certificate at said server machine;

establishing a session from said server machine to a host system on behalf of said client machine, responsive to establishment of said secure session, using a legacy host communication protocol;

passing said stored digital certificate from said server machine to a host access security system, responsive to receiving, at said server machine, a request from said host system for log-on information of said user;

using, by said host access security system, said passed digital certificate to locate access credentials for said user;

returning, from said host access security system to said server machine, a user identifier

associated with said located access credentials and either ~~accessing~~ a stored password or a generated password substitute representing said located credentials; and

forwarding ~~using~~ said ~~stored~~ returned user identifier and password or ~~said generated~~ password substitute from said server machine to said host system as a response to said request for log-on information, such that said forwarded user identifier and password or password substitute can be used by said host system to transparently log said user on to a secure legacy host application executing at said host system, without requiring change to said host system.

Claim 20 (original): The method as claimed in Claim 19, wherein said digital certificate is an X.509 certificate.

Claim 21 (currently amended): The method as claimed in Claim 19 ~~or Claim 20~~, wherein said communication protocol is a 3270 emulation protocol.

Claim 22 (currently amended): The method as claimed in Claim 19 ~~or Claim 20~~, wherein said communication protocol is a 5250 emulation protocol.

Claim 23 (currently amended): The method as claimed in Claim 19 ~~or Claim 20~~, wherein said communication protocol is a Virtual Terminal protocol.

Claim 24 (original): The method as claimed in Claim 21, wherein said host access security system

is a Resource Access Control Facility (RACF) system.

Claim 25 (original): The method as claimed in Claim 19, wherein said server machine is a Web application server machine.

Claim 26 (currently amended): A method for providing end-to-end user authentication for legacy host application access in a computing environment, ~~The method as claimed in Claim 19, further~~ comprising the steps of:

establishing a secure session from a client machine to a server machine using a digital certificate transmitted from said client machine to said server machine, wherein said digital certificate represents said client machine or a user thereof;

storing said transmitted digital certificate at said server machine;

establishing a session from said server machine to a host system on behalf of said client machine, responsive to establishment of said secure session, using a legacy host communication protocol;

automatically sending a log-on message from said client machine to said server machine, responsive to receiving, at said client machine, a request from said host system for log-on information of said user, wherein said log-on message uses placeholder syntax in place of a user identifier and a password of said user;

passing said stored digital certificate from said server machine to a host access security system, responsive to receiving, at said server machine, said log-on message from said client

machine;

using, by said host access security system, said passed digital certificate to locate access credentials for said user;

returning, from said host access security system to said server machine, a user identifier associated with said located access credentials and either a stored password or a generated password substitute representing said located credentials;

modifying, by said server machine, said received log-on message by replacing said placeholder syntax with said returned user identifier and password or password substitute; and

forwarding said modified log-on message from said server to said host system as a response to said request for log-on information, such that said user identifier and password or password substitute from said forwarded log-on message can be used by said host system to transparently log said user on to a secure legacy host application executing at said host system, without requiring change to said host system.

~~requesting by said legacy host application, responsive to said step of establishing said session, log-on information for said user;~~

~~responding to said request for log-on information by sending a log-on message with placeholders from said client machine to said server machine, said placeholders representing a user identification and a password of said user; and~~

~~substituting a user identifier associated with said located access credentials and said stored password or said generated passticket for said placeholders in said log-on message.~~

Claim 27 (canceled)

Claim 28 (new): The method as claimed in Claim 26, wherein said digital certificate is an X.509 certificate.

Claim 29 (new): The method as claimed in Claim 26, wherein said communication protocol is a 3270 emulation protocol.

Claim 30 (new): The method as claimed in Claim 26, wherein said communication protocol is a 5250 emulation protocol.

Claim 31 (new): The method as claimed in Claim 26, wherein said communication protocol is a Virtual Terminal protocol.

Claim 32 (new): The method as claimed in Claim 26, wherein said host access security system is a Resource Access Control Facility (RACF) system.

Claim 33 (new): A method of enabling a user at a client device to transparently log on to a legacy session with a legacy host application, without requiring change to said legacy host application, comprising steps of:

caching a digital certificate associated with said client device, or a user thereof, at a server

to which said digital certificate has been provided for authentication of said client device or said user;

initiating, by said server on behalf of said client device, said legacy session with said legacy host application;

automatically responding, by said client device, to a log-on request from said legacy host application, where said log-on request is sent by said legacy host application responsive to said initiating step, by sending a log-on message in which placeholder syntax is used in place of a user identifier and password expected by said legacy host application; and

before forwarding said sent log-on message from said server to said legacy host application, performing steps of:

using said cached digital certificate to obtain, at said server from a host access security system, said expected user identifier and either said expected password or a password substitute therefor which is generated by said host access security system; and

replacing said placeholder syntax in said sent log-on message with said obtained user identifier and password or password substitute.